EPiC Series in Computing

Volume 93, 2023, Pages 21–32

Proceedings of Society 5.0 Conference 2023

EPiC Computing

Agile Management in Cybersecurity

Petra Maria Asprion[1], Claudio Giovanoli[1], Christopher Scherb[1], Sourabha Bhat[1]

[1] University of Applied Sciences Northwestern Switzerland

petra.asprion@fhnw.ch, claudio.giovanoli@fhnw.ch, christopher.scherb@fhnw.ch, sourabha.bhat@students.fhnw.ch

Abstract

Cybersecurity management has emerged as a topic of growing importance on a global scale. Applying traditional management practices to cybersecurity is often too cumbersome and can lead to significant delays. Today's enterprises must be able to adapt to ever-evolving digital threats and act with corresponding agility and flexibility. Agile methods are well suited for projects without a defined scope, duration, tasks, and resources and has been identified as suitable for meeting the management challenges of cybersecurity teams. Based on an in-depth literature review, this study assumed that adopting an agile approach to cybersecurity helps organisations manage cybersecurity effectively. A first prototypical model was developed and evaluated which combines agile methods with cybersecurity functions - based on a recognized reference model.

Keywords: Agile, Agile Management, Cybersecurity, Frameworks, NIST, Scrum

1 Introduction

Nowadays, from entry-level workers to executives, everyone needs to use technology and digital data to complete daily tasks (Poehlmann et al., 2021). Any networked computer or device is a potential target for a cyber-attack, which could grant access to sensitive data (Weber, 2022). Globally, it is assumed that global cybercrime costs grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025 (Morgan, 2020). Cyberthreats are a high-risk problem due to unpredictability and a growing concern for individuals and organisations using the internet (Yusif & Hafeez-Baig, 2021). White and Daniels (2019) mentioned that cybersecurity is a major management challenge that is escalating across all sectors of the economy and traditional control methods and linear approval processes are insufficient to manage cyber risks. As a result, it is difficult to thoroughly investigate every change with impact on cyber risks that occurs across the organisation. System status and risk are frequently, if not always, out of synchrony with management's knowledge based on internal controls. Therefore, traditional approaches to managing cybersecurity is no longer sufficient due to increased complexity and unpredictability (Weber, 2022).

As a novel approach, agile methods can be potentially used to mitigate this problem because it is a proven set of management practices that enable self-organizing. It lets cross-functional teams to evolve requirements and solutions, which fosters adaptive planning, evolutionary development, early delivery, and continuous improvement (Denning, 2016). Agile provides control, transparency, completed work after each iteration, and continuous customer feedback. In this method, changes or progress is visible to all employees. Hence problems are identified early, and technical debt is minimized.

The current situation described asks for adopting agile for cybersecurity management with the objective that an organisation can manage cybersecurity more effectively. The research question derived is "How can cybersecurity management adopt agile?" along with the corresponding research objective to develop and evaluate an artefact, a model to manage cybersecurity with an agile approach. The remainder of this paper is structured as follows: First the main areas of our research topic derived from the literature is elaborated. Afterwards, selected existing agile methods and cybersecurity frameworks are analysed to determine the gap our solution shall address. The core of our paper describes the iterative development and evaluation of our research artefact. Finally, a conclusion is drawn.

2 Background and Problem Awareness

Due to the ever-changing threat landscape, no cybersecurity program can ever be completely fool proof (McKinsey, 2019). Traditional approaches to cybersecurity management are insufficient to handle evolving threats (Baskerville et al., 2014; He et al., 2022; White & Daniels, 2019)). This is where agile methods come into play: agile methods produce incremental products or procedures on a regular basis. The agile approach facilitates communication between cybersecurity management and other stakeholders, in addition to iterative and continuous delivery. Furthermore, agile permits the definition of requirements both prior to and during execution. This enables earlier detection and resolution of issues, which can be very advantageous for cybersecurity management.

While analysing the literature, it is observed that not only research but also practitioners are discussing adapting agile for cybersecurity can be beneficial (KPMG, 2021; TechTarget., 2022; World Wide Technology, 2018), which outlines the need. Various Studies discusses the application of agile in the field of cybersecurity (Dorca et al., 2016; Fitzer, 2015; He et al., 2022). Kesh and Jane, (2006) apply the fundamentals of agile mechanisms to the field of IT security and recommend the development of security teams and the split of security projects into phases. This gives a general idea of implementing agile to security, but Kesh and Jane (2006) do not mention any standards, or an in-depth description of how agile mechanisms can be applied to security management. Fitzer (2015) discusses the benefits of agile development and its application to information security. He et al. (2022) proposed an agile incident response strategy to manage cyber incidents, where agile principles are used to break processes down into smaller, more manageable chunks, with a focus on specific tasks that can be prioritized and delivered continuously over shorter iterations. But the proposed strategy is only for incidence response, not for whole cybersecurity management.

Many assume cybersecurity is about establishing relevant technology, but it must be clear that security is not just about the technology; the latter is just a part of cybersecurity management (Dawson & Thomson, 2018; Maiorana et al., 2020; Nobles, 2018; Tisdale, 2016). In addition, the human factor, people, either intentionally or accidentally, were responsible for 95% of malware and ransomware attacks (Tripplet, 2022). Zimmermann and Renaud (2019) analysed government, corporate, and hacker-identified cybersecurity issues resulting that the majority are associated with humans. Therefore, organisations have begun to acknowledge that human behaviour is accountable for some of the cyber security problems (Zwilling et al., 2022). According to Yusif & Hafeez-Baig (2021) lack of cybersecurity awareness is one of the leading human weaknesses.

3 Research Approach

As leading research approach the design science research (DSR) was applied; Hevner et al.´s (2004) method can be decomposed in a five steps model as described by Vaishnavi and Kuechler (2015, p. 15): problem awareness, suggestion, development, evaluation, and conclusion. DSR suits very well to the research objective as the outcome of DSR is an evaluated artifact, which can either be a first solution to a problem or an improvement of an existing solution (Hevner and Chatterjee, 2010, p. 5-6).

As first method based on the DSR framework, a literature review was conducted. It entailed key words (agile, cybersecurity, organisation, management, and combinations) using scientific databases (Scopus, Web of science, Science Direct IEEE, ACM, ISACA, Google Scholar), practitioner-oriented contributions (IBM, Swisscom, E&Y, Microsoft, PwC, Cisco, McKinsey, etc.) and standards, frameworks, or best practices form recognised framework providers (e.g., ENISA, ISACA, ISO, NIST). The result was a base to create the first prototypical artefact, the "**Model for Agile Cybersecurity Management**" (M4ACSM). Moreover, the literature review was key to identify and build the artefact upon existing cybersecurity frameworks.

Aligned with Vaishnavi and Kuechler (2015, p. 15) process steps after deriving the problem awareness, the suggestion phase was carried out. The collected and analysed literature from the preceding stage were utilized to conduct an in-depth investigation to collect concrete ideas for developing the framework. An in-depth examination of both research-based and practitioner-based literature on the use of agile in cybersecurity management, following a thorough comprehension of both the agile components and the ´National Institute of Standards and Technology´ cybersecurity framework (NIST CSF) (NIST, 2018), appropriate components were selected as a foundation for agile cybersecurity management. In the development phase, based on the insights from the literature review and foundations from the suggestion phase the M4ACSM artefact was developed. After acquiring a thorough comprehension of agile mechanisms (section 4), the values and principles were adapted to the selected NIST CSF (section 6), which has been selected and used as a foundation. NIST CSF´s core functions (Table 7) were analysed, and four steps were developed to adopt NIST CSF functions in an agile environment (Table 12). In addition, but not in scope of this paper due limited space, awareness and communication as persona approaches were developed to make the artefact people-centric. During the evaluation phase, the M4ACSM was evaluated through a series of interviews with cybersecurity and agile professionals. Based on four selection criteria (expertise area, current job level, experience, size of organisation) five experts with knowledge of both agile and cybersecurity were consulted to evaluate the M4ACSM. Thus, semi-structured interviews were conducted using predefined questions. Table 1 shows the evaluation areas and summarizes relevant expert's opinions.

Evaluation Area	**Summary**
Relevance	• Many firms are implementing organisational changes and adopting agile • Agile cybersecurity management is relevant in the current dynamic situation
Correctness	• Agreement of the approach and structure of M4ACSM, enhancements desired
Usability	• Ideally applicable to all organisations sizes, but culture can be a bottleneck • The M4ACSM can be used with modifications per organisational needs • With this approach, reusable components can be beneficial • All experts said that the artefact is easily understandable
Missing Elements	• Team dependency • Risk stories would be helpful • Recommendation for modifying the M4ACSM aligned with framework update(s)

Table 1: Evaluation areas and all expert's opinions

4 Agile Mechanisms

Beck et al. introduced in 2001 agile mechanisms using the ´Agile Manifesto´ of software engineering. These mechanisms served as foundation to develop the M4ACSM (Section 6). Implementing agile practices ensures the 'doing agile' part but to move from doing agile to being agile, it is important to incorporate agile values, principles and practices which emphasize a people-centric, collaborative approach (*Agile Alliance*, n.d.). Teams who commit to ´being agile´ agree to take responsibility for their work, be willing and able to deal with uncertainty, and work toward continuous improvement (Horlach & Drechsler, 2020). ´Agile´ consists of three hierarchical layers: four agile values, twelve agile principles and numerous agile practices; the values and principles do not establish rules but rather reflect the appropriate attitude for agile practices (Schön et al., 2015).

4.1 Agile Values and Principles

While interpreting the Agile Manifesto (Beck et al., 2001), it is important to view the agile principles as a pair of values that cannot or should not exist alone. The four agile values are: (1) individuals and interactions over processes and tools, (2) working software over comprehensive documentation, (3) customer collaboration over contract negotiation, (4) responding to change over following a plan. After considering the agile values it is essential to focus on the twelve agile principles outlined in Table 2.

#	**Twelve Agile Principles – shortened and generalized**
1	Highest priority is to satisfy the customer through the early and continuous delivery
2	Welcome changing requirements, even late in development
3	Deliver frequently, from a couple of weeks to a couple of months, with a preference for a shorter timescale
4	The most efficient and effective method of conveying information to is face-to-face conversation
5	Business people and developers must work together daily throughout the project
6	Build projects around motivated individuals. Give them the environment and support them
7	Working software is the primary measure of progress
8	Agile processes promote sustainability
9	Continuous attention to technical excellence and good design enhances agility
10	Simplicity, the art of maximizing the amount of work not done, is essential
11	The best architectures, requirements, and designs emerge from self-organizing teams
12	At regular intervals, the team reflects on how to become more effective, then tune behaviour accordingly

Table 2: Twelve agile principles (adopted from Agile Manifesto, Beck et al, 2001).

4.2 Agile Practices

Agile practices incorporate agile values and principles. There are various agile approaches, such as ´Kanban´, ´Scrum´, ´Extreme programming´ etc. all of these methods use agile elements, but each method has its own life cycle, roles, benefits, and drawbacks (Ozkan et al., 2020). In this research, based on developed criteria, Scrum was used to align agile cybersecurity management (Table 3).

#	**Four Agile Practices criteria based on Scrum – generalized**
1	**Divide**: each project should be divided into a smaller set of manageable and comprehensible components that are shared throughout the teams, to enhance communication and shared knowledge
2	**Transparency**: the team has access to all information, including communication and comments from the product owner, through the various meetings held throughout the development process
3	**Self-organisation**: everyone shares the responsibilities
4	**Self-retrospective**: Self-assessment of achieved versus necessary goals after each iteration/sprint

Table 3: Four agile practices criteria

The scrum team and related ´scrum´ roles are vital to organize an agile team organisation to manage cybersecurity in an agile way; it consists of roles (Table 4), procedures (Table 5) and artifacts (Table 6).

Roles	Description
Scrum master	Helps everyone in the team and organisation to understand scrum and is responsible for the effectiveness of the scrum team. • Training team for self-management and training organisation for scrum adoption • Removing impediments to achieving the (pre)-defined goals • Facilitating collaboration and communication • Helping product owner in defining backlog items
Product owner	Responsible for the value of the product, with the help of the scrum team and responsible for: • Creating and communicating product vision • Product backlog management includeng backlog items and prioritization • Ensuring clarity, and transparency about backlog items
Developers	Team members, responsible for the development of any aspect of usable in each sprint • Responsible for the creation of sprint backlog and sprint planning • Adapting their plan towards the sprint goal, adhering to the definition of done

Table 4: Scrum roles

Procedures	Description
Product vision	Serves as the purpose and focus of a project or committed goal. It defines the objectives, and it is necessary that the entire scrum team understands, shares, and works toward the same vision. It is developed by the product owner in collaboration with other relevant stakeholders and serves as a guide for the scrum team.
Sprint	Fixed length of the event of one month or less. A new sprint starts after the conclusion of the previous sprint. All the work necessary to achieve goals, sprint planning, daily scrums, sprint review and retrospectives takes place during a sprint. It is possible to refine the product backlog as needed; the scope can be clarified and re-negotiated with the product owner.
Burndown chart	Shows how much work is remaining in a sprint. This helps the scrum team to see the number of hours remaining, and how much work is already done. The scrum master maintains it.
Scrum events	Container for all the events that happen in a sprint. Each of these events is an occasion to evaluate and modify scrum items. This enables transparency throughout the process.

Table 5: Scrum procedures

Artefact	Description
Product backlog	It is the only source of all work to be undertaken by the scrum team. It contains product vision which gives the 'to be' state of a product/end goal of a product. It contains all desired product features. Each item in the product backlog should map to a clear business value. This list can contain non-functional items or bugs as well.
Sprint backlog	Comprises the sprint goal, a set of items from the product backlog and an actionable plan for delivering the increment. The scrum team is responsible for creating it.

Table 6: Scrum artefacts

5 Cybersecurity Frameworks

5.1 Preliminary Considerations

A cybersecurity framework is a set, a collection of guidelines, recommendations that organisations adhere to be better prepared to govern and manage cybersecurity. Such frameworks often incorporate a selection of relevant standards, methodologies, procedures, and processes that align policies, business, and technology responses (Syafrizal et al., 2022). It is important to choose the ´right´ framework that aids in effective cybersecurity management (Dedeke & Masterson, 2019). Syafrizal et al. (2022) discovered more than 250 frameworks available globally, which include international standards like NIST´s CSF, ISACA´s COBIT, ISO/IEC standards, industry specific frameworks like HIPAA, or local regulations like the ´General Data Protection Regulation´ (GDPR), which also influences cybersecurity management. The choice of the ´right´ cybersecurity framework that an organisation makes may be influenced by a wide range of factors. For example, the industry requirements, the regulatory requirements, as well as resources and budget. ISO/IEC standards are useful when a firm must show its information/cybersecurity capabilities via e.g., an ISO/IEC 27001/2 certification. However, implementing ISO/IEC standards can be time-consuming and expensive (Roy, 2020).

The NIST CSF (NIST CSF, 2018) is a voluntary guideline from the U.S. which can help organisations to establish cybersecurity from a management or top-down perspective. According to what is stated in the NIST CSF, organisations of any size can use NIST CSF to develop cybersecurity, and they are able to use NIST CSF in addition to any other frameworks that are already in place. NIST CSF is well categorized; also, it maps subcategories to other frameworks like CIS CSC, COBIT, and ISO/IEC 27001/2. The following benefits of using NIST CSF are derived from different studies (Dedeke & Masterson, 2019; Roy, 2020; Powell et al., 2022; Syafrizal et al., 2022): (1) technology independence, (2) gives direction for the organisation, not just for the IT department, (3) facilitates and improves executive, business, and operational layer communication, (4) well structured, easy to implement at the organisational level, (5) user friendly (6) streamlined for higher management, (7) predefined ´profiles´ help organisations to define current and future profiles of their organisation, (8) references to other frameworks.

5.2 NIST CSF Components

After a comparison of cybersecurity related frameworks, the NIST CSF (2018) was chosen as the leading framework to create the M4ACSM prototype. The NIST CSF consist of three components:

Profiles: the framework profiles are an alignment of the organisation's business requirements, risk tolerance, and resources with the framework's functions, categories, and subcategories. The profile aligns standards, guidelines, and practices with the framework core for a specific implementation situation. To construct a profile, an organisation can analyse all categories and subcategories and decide which are most important based on business/mission drivers and a risk assessment.

Tiers: the framework ´tiers´ demonstrate how an organisation views cybersecurity risk and address it. Tiers indicate the degree to which an organisation's cybersecurity risk management practices exhibit the framework's characteristics (e.g., risk and threat aware, repeatable, and adaptive). The tiers describe how an organisation practices over a range, from partial (Tier 1) to adaptive (Tier 4). These tiers show the progression from informal, reactive responses to flexible and risk-aware approaches.

Core: the framework ´core´ is a collection of cybersecurity activities and relevant references. The core is comprised of four components: functions, categories, subcategories, and informative references. The core's highest level comprises functions, which are ´Identity´, ´Protect´, ´Detect´, ´Respond´, and ´Recover´. Table 7 describes the five functions and (some selected) related categories.

Function (description abridged)	**Category (selection)**
Identify: understanding how to manage cybersecurity risks	Asset Management, Business Environment, Governance, Risk Assessment, Risk Management Strategy, …
Protect: develop and implement the required safeguards	Identity Management & Access Control, Awareness & Training, Data Security, …
Detect: implement required activities to detect the occurrence of a cybersecurity event	Anomalies And Events, Security Continuous Monitoring, Detection Processes
Respond: implement relevant activities in response to an identified cybersecurity incident	Response Planning, Communications, Analysis, Mitigation, Improvements
Recover: implement activities required to maintain resilience plans & restore capabilities	Recovery Planning, Improvements, Communications

Table 7: NIST CSF core functions (NIST CSF, 2018)

5.3 NIST Implementation

The following seven implementation steps (Table 8) describe how the NIST CSF can be used by an organisation to create a cybersecurity program or to improve an existing one. These steps can be repeated as necessary to improve an organisation's cybersecurity management. Progress can be tracked through iterative revisions, which can then be compared to the target profile. These realization steps and related deliverables can be used to align the existing cybersecurity management with agile methods.

Implementation steps	Deliverables
(1) Prioritize and scope	Cybersecurity program scope
(2) Orient	List of threats and vulnerabilities
(3) Create relevant profile	Current profile
(4) Conduct the risk assessment	Current risk profile
(5) Create the target profile	Target profile
(6) Determine, analyse, and prioritize gaps	Gap analysis report
(7) Implementation action plan	Action plan

Table 8: Implementation steps adapted from NIST CSF (NIST CSF, 2018)

6 Model for Agile Cybersecurity Management

To develop the M4ACSM**,** agile values, principles and agile practices were adopted for the application in cybersecurity management. We approached for the prototype four steps:

(1) adoption of agile values and principles for cybersecurity (resulted in Table 9 and 10),
(2) mapping of the derived values and principles (Table 9 and 10) to cybersecurity management responsibilities to demonstrate their application (Table 11),
(3) derivation of four steps to add NIST CSF functions to the agile backlog (Table 12),
(4) mapping of the implementation steps from NIST CSF (Table 8) to agile practices.

6.1 Agile Values, Principles and Practices

The agile values (Table 9), agile principles (Table 10), and agile practices with focus on relevant roles and responsibilities (Table 11) were adapted to cybersecurity management.

#	Agile Cybersecurity Values for Cybersecurity Management
1	Individuals and interactions over processes and tools in cybersecurity management
2	Practising cybersecurity management than comprehensive documentation
3	Collaborating with relevant stakeholders and the organisation is seen as a customer
4	Reacting to change rather than following a plan

Table 9: Agile values mapped to cybersecurity management

#	Agile Cybersecurity Principles for Cybersecurity Management
1	Enhancing security and customer satisfaction through timely and continuous delivery of results
2	Be adaptable to changing priorities and needs and see this change as an opportunity to improve security. Agile processes harness change to give customers (internal/external) a competitive advantage
3	In a rapidly changing environment, plan and operate in short time intervals to allow for enough flexibility and adaptability
4	Cybersecurity management must collaborate continuously with all relevant stakeholders. This teamwork ensures a more acceptable solution
5	Build the team with driven and competent individuals. Provide them with the necessary environment and support, and have faith in their ability to complete the job
6	Build the team with driven and competent individuals. Provide them with the necessary environment and support, and have faith in their ability to complete the job

7	The most significant progress and the ultimate objective is to create cybersecurity management that adds value to the organisation
8	The agile process promotes sustainable work. The team and stakeholders should be able to maintain a steady pace indefinitely to ensure effective results
9	Continuous focus on quality, as well as user requirements, promotes acceptance of cybersecurity measures by the stakeholders and organisation
10	Simplicity: The avoidance of excessive documentation, complexity, and high effort is essential
11	Self-organising teams provide the finest ideas, solutions, and outcomes
12	The team and other associated stakeholders periodically reflect on how to build more effective Cybersecurity management. This enables continuous improvement

Table 10: Agile cybersecurity principles mapped to cybersecurity management

Creating the product vision provides the agile cybersecurity management team with clear direction and structure which can increase the motivation of all stakeholders involved. In addition, business goals remain crucial for the organisation as they determine the actual benefits of an agile cybersecurity management team for the business. This promotes the core principle of the agile mindset, which prioritizes providing customers with value-added services. The product vision of the agile cybersecurity management team should be aligned with organisational objectives; therefore, (top) management and key stakeholders should be providing the vision to guarantee that organisational requirements are addressed.

#	**Roles**	**Agile Cybersecurity Practices –** **Responsibilities for the cybersecurity management team**
1	All roles (Product Owner, Scrum Master, Development Team)	- all individuals in the organisation responsible for organisational security - the organisation acts as a customer, which comprises all key stakeholders - as an interdisciplinary team, the team must have all skills related to cybersecurity management to enable decision-making and self-organized work - continuously identify and upgrade the skillsets by undergoing necessary training
2	Product Owner	- for the entire product backlog, accountable for cybersecurity management - decides on what product backlog should contain and their prioritization - take all relevant suggestions from relevant stakeholders of an organisation by collaborating with them. The product owner can list and prioritize tasks in the product backlog - has cybersecurity knowledge with decision-making power in an organisation - active involvement of the product owner is needed where he/she has tasks in terms of cybersecurity management
3	Development Team	- the development team should consist of a minimum of three and a maximum of nine members to provide an efficient, agile process
4	Scrum Master	- plays the same role as originally intended, as this job is to assist in the execution of agile principles, rules, and practices - If he/she possesses some background knowledge in the cybersecurity area, he/she can support the scrum team in an agile way of working - plays a key advocate role for agile cybersecurity management within the organisation because among other things, he/she improve awareness and knowledge of the agile methods among participants

Table 11: Roles and responsibilities for the cybersecurity management team

The product backlog is the key instrument for agile cybersecurity management, where all requirements are mapped in prioritized order. It begins with known requirements and is continuously developing and adapting to new conditions. All necessary tasks for the establishment, operation, and further development of cybersecurity management should be listed, as well as additional measures coming from risk analysis results. The product backlog is the only source of cybersecurity management requirements and is therefore a fundamental starting point for establishing, implementing, maintaining, and enhancing cybersecurity management in compliance with standards and (internal) policies.

Product backlog entries can come from all stakeholders of an organisation. The product owner decides which requirements to include and how to prioritize them. Especially during initial creation, considering NIST CSF (2018), it must be ensured that the components of the framework are not simply accepted, instead by analysing the current state of the organisation and by considering previously established elements (e.g., other frameworks, standards, procedures, etc.). Cybersecurity management is highly changing; hence new requirements might arise because of new threats or risk analysis, and lesson learned. In agile cybersecurity management addition of new requirements at any time plays a crucial role. When a new requirement arises, the product owner focus on the adaption of the backlog and reprioritizing them.

6.2 Agile and NIST CSF Combined

The NIST CSF (2018) is recognized as a sufficient framework for implementing and executing cybersecurity management and provides various benefits (section 5.1). This makes it an ideal foundation for a combination with Agile/Scrum to develop the first prototype of the M4ACSM. Therefore, for the first M4ACSM (Figure 1), we combined the NIST CSF with Agile/Scrum by adding the NIST CSF core functions (Table 7), the NIST CSF´s implementation steps (Table 8) with agile procedures (Table 5) and artefacts (Table 6).

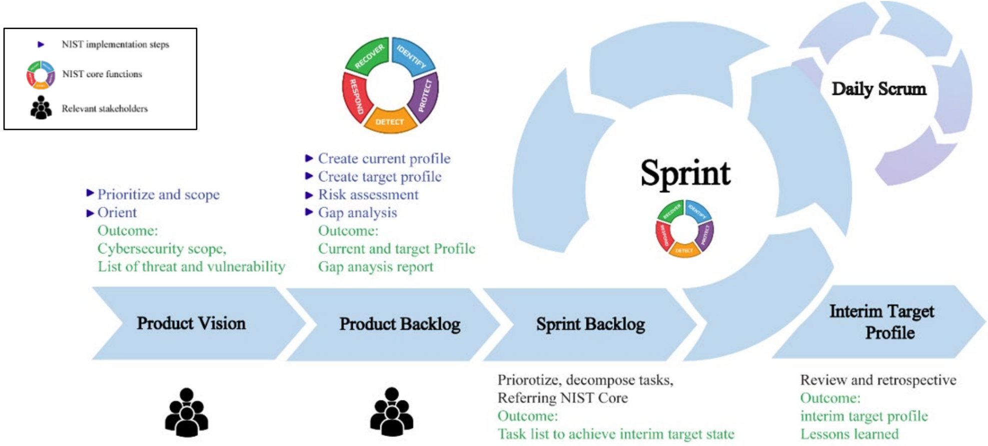

Figure 1: Model for Agile Cybersecurity Management (M4ACSM)

Regarding a cybersecurity management team, it is recommended that the team performs for each NIST CSF (2018) function the four steps as outlined in Table 12. Although Table 12 is not exhaustive, it provides a sense of how these four steps work and should be carried out for the five NIST CSF core functions and related categories (Table 7).

When selecting the core functions from the NIST framework, the following steps can be beneficial for the organisation: firstly, identify and analyse the (most) relevant functions for cybersecurity management. Secondly, the identified functions must be further subdivided into subcategories based on the organisation´s needs (e.g., decomposing asset management into hardware and software assets). Third, prioritizing these tasks and adding them to the product backlog. Lastly, the functions should be improved continuously (e.g., incorporating feedback and lessons learned during each sprint). In addition, the agile values, principles, and practices (section 6.1, 6.2) adopted for cybersecurity should be applied by the cybersecurity management team as guiding principles to continuously deliver effective cybersecurity in an agile environment.

Functions	**Four steps for an Agile Cybersecurity Management (per NIST core function)**

Identify	**Identify and analyse**: All assets (physical, software), data flow, current roles, policies, legal, regulatory requirements, risk management, collaboration/communication with stakeholders **Decompose**: the task based on organisation needs **Prioritize**: tasks and add them to the product backlog **Continuous improvement**: monitor central asset inventory, central threat inventory, risk management process etc., after each sprint, add inputs from lessons learned
Protect	**Identify and analyse**: access control, access management strategy, user authentication, training and awareness practices, data flow, data management protection **Decompose**: the task based on organisation needs **Prioritize**: tasks and add them to the product backlog **Continuous improvement**: continuously monitor data protection, access management, incidence response plans, and asset maintenance consistent with the policies and regulations
Detect	**Identify and analyse**: network operations and expected dataflow, detected event analysis, continuous monitoring of security, detection process **Decompose**: the task based on organisation needs **Prioritize**: tasks and add them to the product backlog **Continuous improvement**: detection process and event analysis, lessons learned improvement
Respond	**Identify and analyse**: incidents, processes to receive and analyse vulnerabilities **Decompose**: the task based on organisation needs **Prioritize**: tasks and add them to the product backlog **Continuous improvement**: improve response plan based on lessons learned
Recover	**Identify and analyse**: recovery plan, restoring communication with relevant stakeholders **Decompose**: the task based on organisation needs **Prioritize**: tasks and add them to the product backlog **Continuous improvement**: improve recovery plan based on lessons learned

Table 12: NIST CSF core functions with exemplary agile cybersecurity management steps

The agile procedure product vision (Table 5) is the starting point of agile cybersecurity management, where along with relevant stakeholders, the cybersecurity team performs the first two by NIST CSF recommended steps (Table 8): (1) **Prioritise and scope** and (2) **Orient**: The cybersecurity team and stakeholders align together objectives at the organisational level, the scope of the system and assets in an organisation, the statutory and regulatory requirements, assets (hardware, software, human capital), finance, and management resources. After defining the scope and listing threats and vulnerabilities, the product vision can be created, and the modified vision is suitable for cybersecurity management.

With the newly modified product vision the product owner, along with relevant stakeholders, performs step three from NIST CSF implementation step (3) **Create the current profile**: Determining the current cybersecurity management state, indicating which category and subcategories from the NIST CSF are currently achieved is the next step. NIST CSF functions can help to determine cybersecurity management's status. By analysing business objectives, environment, and risk appetite, an organisation can prepare the current profile and performing the fourth step: (4) **Conduct the risk assessment**: Performing an overall risk management assessment. The operational environment will be analysed considering the likelihood of a cybersecurity event and the related impacts on the business. The fifth step is (5) **Create the target profile**: This means that a target profile needs to be developed based on the NIST CFS functions describing the organisation's desired cybersecurity profile while considering external stakeholders and then performing the next step (6) **Determine, analyse, and prioritise gaps**: By comparing the current profile to the target profile, identify the resources necessary to close the gaps. An action plan considering the prioritised gaps will identify costs, benefits, and risks to accomplish the results in the target profile. And then performing the last step (7) **Implement the action plan**: All defined tasks will all be added to the cybersecurity backlog; the backlog will be prepared by the cybersecurity team, where the team selects the task for the current sprint. These tasks can be further decomposed as needed. After this, a sprint takes place, which involves sprint planning and execution, and the team can decide the frequency of the meetings needed. The deliverable of the sprint will be the interim target profile.

7 Conclusion

Because of the rapid growth of threats, cybersecurity management is a key management challenge that is spreading across all industries. To create agile cybersecurity management standards, first, the benefits of Agile over traditional management approaches, as well as circumstances when agile practices are advantageous, were analysed. Furthermore, the benefits of the chosen NIST CSF were examined. While reviewing the literature, it became evident that not just technological solutions but also a people-centred approach are required for cybersecurity management – these fits well with agile mechanisms.

The developed prototypical artefact M4ACSM aims to provide a guideline, a first process-oriented approach for implementing or improving cybersecurity management in an organisation. The recommendations give a flexible approach by integrating agile and the NIST CSF. The prototype was evaluated by experts who agreed on the various components and offered additional insights which could be iteratively added to the artefact. This assessment helped to understand and incorporate possible improvements to the artifact. The final artefact can be utilized by businesses as a starting point to satisfy cybersecurity management requirements and provide them with a state of preparedness in a dynamic threat environment. Because of the current research's scope and limits, there are many additional aspects of this topic that future research can investigate. Scrum, a commonly used agile practice, was used for this research but also other agile methods such as Kanban or SAFe 6.0 can serve as a basis. Because of the benefits outlined, only the NIST CSF was detailed examined and aligned in this research. This, however, can be utilized with different standards/frameworks may be to better align the agile framework with other existing organisational approaches. Furthermore, how to handle standard updates or team reliance can also be considered in further research.

References

Agile Alliance. (n.d.). https://www.agilealliance.org/agile101/agile-glossary

Baskerville, R., Spagnoletti, P., Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information and Management*, *51*(1). https://doi.org/10.1016/j.im.2013.11.004

Beck, K., Beedle, M., van Bennekum, A., Cockburn, A., Cunningham, W., Fowler, M., Grenning, J., Highsmith, J., Hunt, A., Jeffries, R. (2001). *The Agile Manifesto*. www.agilemanifesto.org

NIST CSF (2018) Framework for Improving Critical Infrastructure Cybersecurity. https://doi.org/10.6028/NIST.CSWP.04162018

Dawson, J., Thomson, R. (2018). The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. In *Frontiers in Psychology* (Vol. 9, Issue JUN). https://doi.org/10.3389/fpsyg.2018.00744

Dedeke, A., & Masterson, K. (2019). Contrasting cybersecurity implementation frameworks (CIF) from three countries. *Information and Computer Security*, *27*(3). https://doi.org/10.1108/ICS-10-2018-0122

Denning, S. (2016). How to make the whole organization "Agile." In *Strategy and Leadership* (Vol. 44, Issue 4). https://doi.org/10.1108/SL-06-2016-0043

Dorca, V., Munteanu, R., Popescu, S., Chioreanu, A., & Peleskei, C. (2016). Agile approach with Kanban in information security risk management. *2016 20th IEEE International Conference on Automation, Quality and Testing, Robotics, AQTR 2016 - Proceedings*. https://doi.org/10.1109/AQTR.2016.7501278

Fitzer, J. R. (2015). Agile Information Security Using Scrum. *Journal of Systems and Information Technology*, *2*(3).

He, Y., Zamani, E. D., Lloyd, S., Luo, C. (2022). Agile incident response (AIR): Improving the incident response process in healthcare. *International Journal of Information Management*, *62*. https://doi.org/10.1016/j.ijinfomgt.
2021.102435

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly: Management Information Systems*, *28*(1). https://doi.org/10.2307/25148625

Horlach, B., Drechsler, A. (2020). It's not easy being agile: Unpacking paradoxes in agile environments. *International Conference on Agile Software Development*, *396 LNBIP*, https://doi.org/10.1007/978-3-030-58858-8_19

KPMG. (2021). *The seven ways of the agile CISO*. https://home.kpmg/xx/en/home/campaigns/2019/07/the-seven-ways-of-the-agile-ciso.html

Maiorana, F., Csizmadia, A. P., & Richards, G. M. (2020). Managing data and projects: Lessons learnt from comparing computing curricula. *Proceedings of 2020 IEEE International Conference on Teaching, Assessment, and Learning for Engineering, TALE 2020*. https://doi.org/10.1109/TALE48869.2020.9368420

McKinsey. (2019). Perspectives on transforming cybersecurity. *McKinsey Global Institute*, *32*(March).

Morgan, S. (2020). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Cybercrime Magazine. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021

Nobles, C. (2018). Botching Human Factors in Cybersecurity in Business Organizations. *HOLISTICA – Journal of Business and Public Administration*, *9*(3). https://doi.org/10.2478/hjbpa-2018-0024

Ozkan, N., Gok, M. S., Kose, B. O. (2020). Towards a Better Understanding of Agile Mindset by Using Principles of Agile Methods. *Proceedings of the 2020 Federated Conference on Computer Science and Information Systems, FedCSIS 2020*. https://doi.org/10.15439/2020F46

Poehlmann, N., Caramancion, K. M., Tatar, I., Li, Y., Barati, M., Merz, T. (2021). *The Organizational Cybersecurity Success Factors: An Exhaustive Literature Review*. https://doi.org/10.1007/978-3-030-71017-0_27

Powell, M., Brule, J., Pease, M., Stouffer, K., Tang, C., Zimmerman, T., Deane, C., Hoyt, J., Raguso, M., Sherule, A., Zheng, K., & Zopf, M. (2022). *Protecting Information and System Integrity in Industrial Control System Environments*. https://doi.org/https://doi.org/10.6028/NIST.SP.1800-10

Roy, P. P. (2020). A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard. *2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications, NCETSTEA 2020*. https://doi.org/10.1109/NCETSTEA48365.2020.9119914

Schön, E. M., Escalona, M., Thomaschewski, J. (2015). Agile Values and Their Implementation in Practice. *International Journal of Interactive Multimedia and Artificial Intelligence*, *3*(5), 61. https://doi.org/10.9781/IJIMAI.2015.358

Syafrizal, M., Selamat, S. R., & Zakaria, N. A. (2022). Analysis of Cybersecurity Standard and Framework Components. *International Journal of Communication Networks and Information Security*, *12*(3). https://doi.org/10.17762/ijcnis.v12i3.4817

TechTarget. (2022). *Build an agile cybersecurity program with Scrum*. https://www.techtarget.com/searchsecurity/tip/Build-an-agile-cybersecurity-program-with-Scrum

Tisdale, S. M. (2016). Architecting a Cybersecurity Management Framework: Navigating and Traversing Complexity, Ambiguity, and Agility. *ProQuest Dissertations and Theses*, *May 2016*.

Tripplet, W. (2022). Addressing human factors in cybersecurity. *Journal of Cybersecurity and Privacy*, *2*(3), 573–586.

Vaishnavi, V. K., Kuechler, W. (2007). Design science research methods and patterns: Innovating information and communication technology. In *Design Science Research Methods and Patterns: Innovating Information and Communication Technology*. https://doi.org/10.1201/9781420059335

Weber, K. (2022). Cybersecurity and ethical, social, and political considerations: when cybersecurity for all is not on the table. *Humanities and Social Sciences*, *29*(1), 87–95.

White, J., & Daniels, C. (2019). Continuous cybersecurity management through blockchain technology. *2019 IEEE Technology and Engineering Management Conference, TEMSCON 2019*. https://doi.org/10.1109/TEMSCON.2019.8813712

World Wide Technology. (2018). *Adopting Agile Principles in Cybersecurity*. https://www.wwt.com/article/adopting-agile-principles-cybersecurity

Yusif, S., & Hafeez-Baig, A. (2021). A Conceptual Model for Cybersecurity Governance. *Journal of Applied Security Research*, *16*(4). https://doi.org/10.1080/19361610.2021.1918995

Zimmermann, V., & Renaud, K. (2019). Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. *International Journal of Human Computer Studies*, *131*. https://doi.org/10.1016/j.ijhcs.2019.05.005

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, *62*(1). https://doi.org/10.1080/08874417.2020.1712269